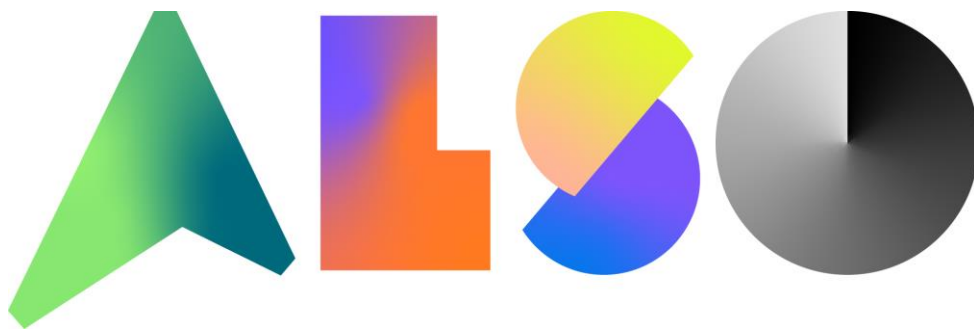


How to Fortinet

Konfiguration SSL-VPN im Tunnelmodus

Version 1.0





Inhaltsverzeichnis

EINFÜHRUNG.....	3
BENUTZERKONTEN UND GRUPPEN KONFIGURIEREN	4
User und Gruppen in der CLI konfigurieren:	5
Adressenobjekte in der CLI konfigurieren:	6
SSL VPN PORTALE KONFIGURIEREN	6
Konfigurieren der SSL-Portale über die CLI:	9
SSL-VPN SETTINGS	9
Konfigurieren der SSL-VPN Settings in der CLI:	12
FIREWALL REGELN KONFIGURIEREN	13
Firewallregel in der CLI konfigurieren:	15
VPN CLIENT KONFIGURIEREN	15
KONTROLLEN UND LOGS:	17



Einführung

Um ein SSL-VPN von Anfang an aufzubauen muss man folgende vier Punkte konfigurieren:

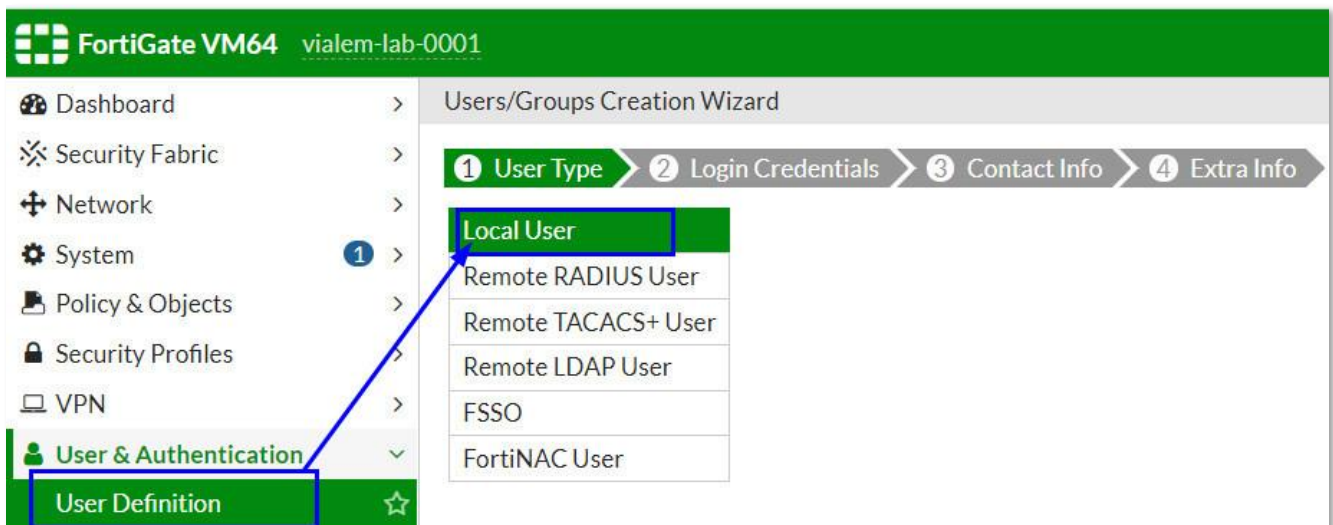
1. Einrichten Benutzerkonten und Gruppen für die remote SSL-VPN Benutzer
2. SSL-VPN Portale konfigurieren
3. SSL-VPN Einstellungen konfigurieren
4. Firewall Regeln konfigurieren

Am besten konfiguriert man vorab alle Adressen Objekte, User und Gruppen Objekte. So kann man danach in einem Zug durchkonfigurieren.

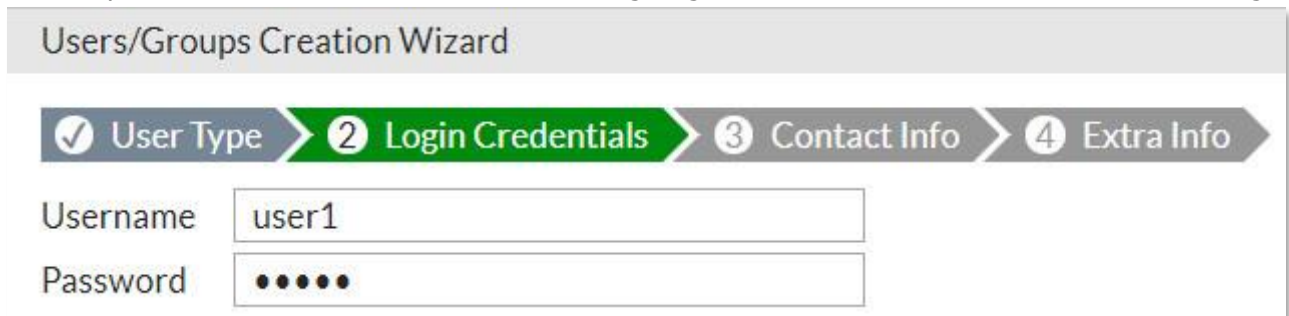
Benutzerkonten und Gruppen konfigurieren

In unserem Beispiel werden wir die User lokal auf der FortiGate konfigurieren. Man hat aber auch die Möglichkeit über LDAP, Radius die User anzubinden.

1. Über das *Menu User & Authentication* → *User Definition* kommt man in das Menu um die User anzulegen
2. Für einen Lokalen User anzulegen wird beim User Type *Local User* ausgewählt



1. Username definieren
2. Passwort definieren.
3. Optional kann auch ein FortiToken hinzugefügt werden für die 2Factor Authentifizierung

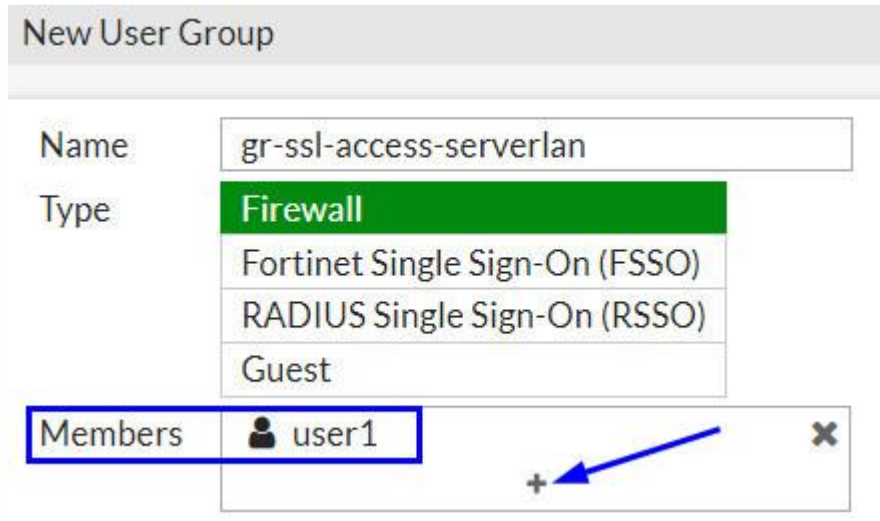


The screenshot shows the 'Users/Groups Creation Wizard' at the 'Login Credentials' step. The progress bar shows 'User Type' as completed and 'Login Credentials' as the current step. The 'Username' field contains 'user1' and the 'Password' field is masked with dots.

Wenn alle User angelegt sind, kann eine UserGruppe definiert werden:

[https://fortinet.also.ch/wiki/index.php?title=FortiGate:FAQ#User .2F Gruppe](https://fortinet.also.ch/wiki/index.php?title=FortiGate:FAQ#User_.2F_Gruppe)

In unserem Beispiel werden wir die Gruppe *gr-ssl-access-serverlan* nennen und den Benutzer *user1* hinzufügen



User und Gruppen in der CLI konfigurieren:

User konfigurieren:

```
config user local
  edit "user1"
    set type password
    set passwd [PASSWORT]
  next
end
```

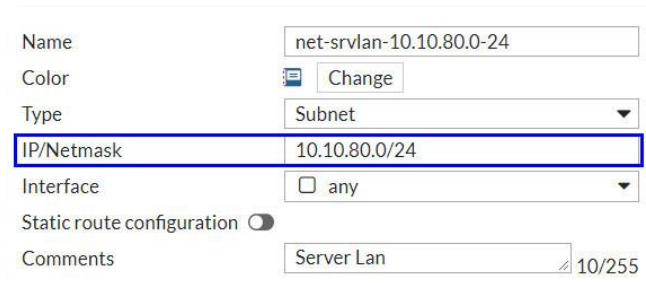
Usergruppe konfigurieren:

```
config user group
  edit "gr-ssl-access-serverlan"
    set member "user1"
  next
end
```

Nun definieren wir Netzwerkobjekte, welche wir danach für den Aufbau des SSL-VPN brauchen:

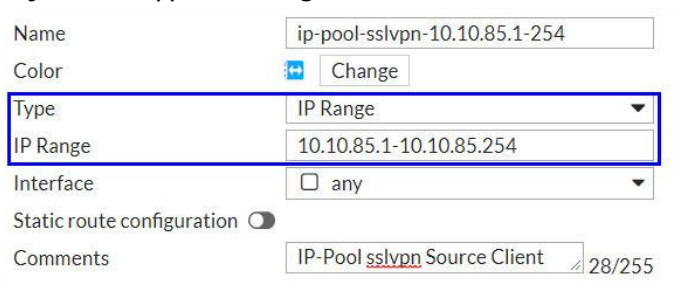
Serverlan (Netz welches durch das VPN erreicht werden soll:

Ein Objekt wird über das Menu Policy & Objects → Addresses →  **Create New** eröffnet:



Adressenobjekt für den **IP Pool**.

Der IP Pool definiert die IP Adresse welche dem Client von der FortiGate zugewiesen bekommt. Hier wird das Adressenobjekt als Type IP Range benutzt:



The screenshot shows the configuration window for a new address object. The 'Name' field is 'ip-pool-sslvpn-10.10.85.1-254'. The 'Color' field has a 'Change' button. The 'Type' dropdown is set to 'IP Range'. The 'IP Range' field contains '10.10.85.1-10.10.85.254'. The 'Interface' dropdown is set to 'any'. The 'Static route configuration' toggle is turned off. The 'Comments' field contains 'IP-Pool sslvpn Source Client'.

Adressenobjekte in der CLI konfigurieren:

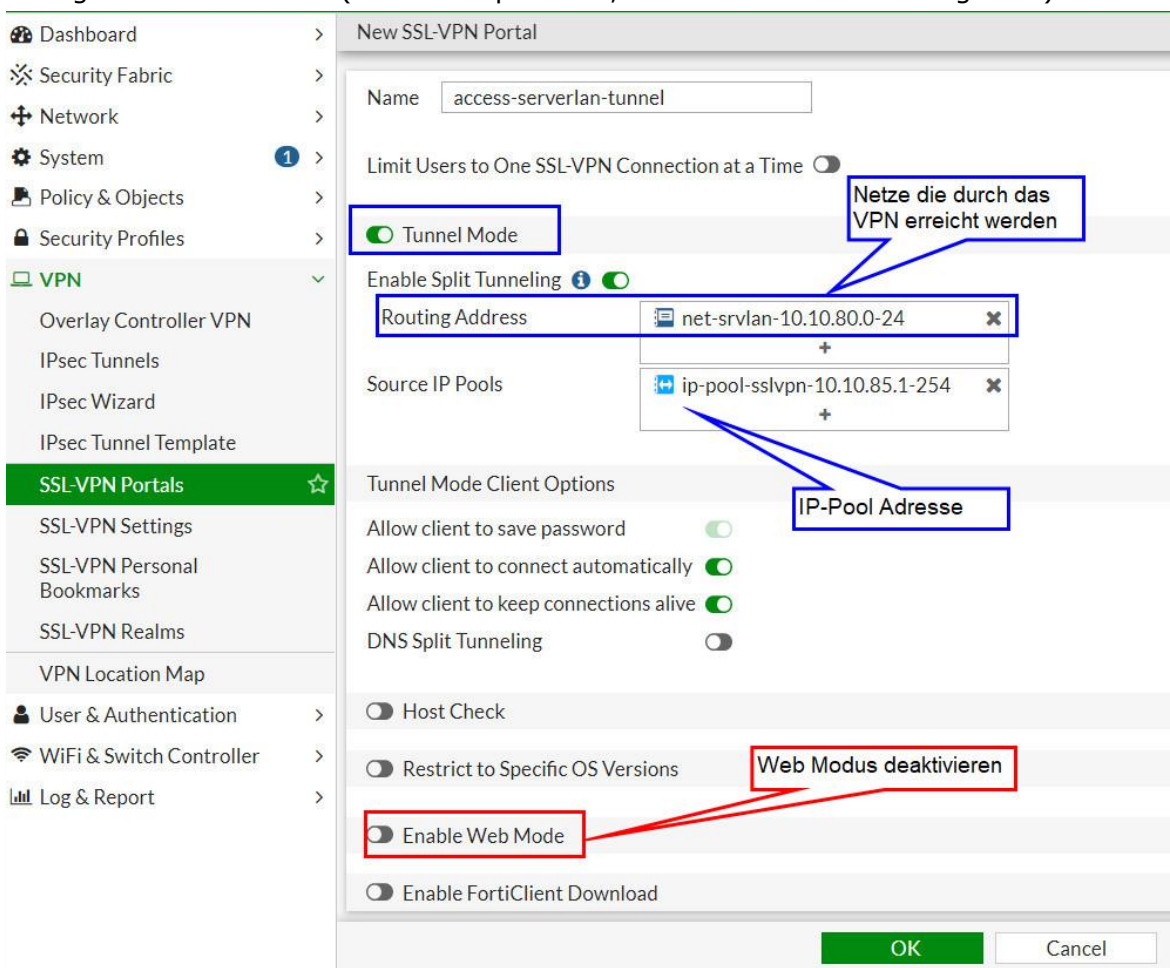
```
config firewall address
  edit "net-srvlan-10.10.80.0-24"
    set comment "Server Lan"
    set color 2
    set subnet 10.10.80.0 255.255.255.0
  next
  edit "ip-pool-sslvpn-10.10.85.1-254"
    set type iprange
    set comment "IP-Pool sslvpn Source Client"
    set color 18
    set start-ip 10.10.85.1
    set end-ip 10.10.85.254
  next
end
```

SSL VPN Portale konfigurieren

Wir wollen ein SSL-VPN im Tunnel Modus konfigurieren. Das heisst, wir brauchen für die Verbindung einen VPN Client welchem von der Fortigate her eine IP Adresse zu einem virtuellen Netzwerkatapter zugewiesen wird. Es gibt bereits drei vordefinierte Portale. In unserem Beispiel werden wir aber ein eigenes anlegen und auf unsere Bedürfnisse konfigurieren. Wir konfigurieren einen Split tunnel (es werden nur die IP Adressen in den Tunnel geroutet welche wir explizit definieren. Was genau ein Split Tunnel ist wird in diesem Wiki Artikel genauer erläutert: https://fortinet.also.ch/wiki/index.php?title=FortiGate:FAQ#Was_versteht_man_beim_SSL-VPN_unter_einem_Split-Tunnel.3F

Um das Portal zu konfigurieren über das Menu *VPN* → *SSL-VPN Portals* → [+ Create New](#)

1. Portal Name definieren (Im Feld *Name*)
2. Tunnel Modus anwählen. Den Schalter *Enable Web Mode* deaktivieren
3. Die Option *Enable Split Tunneling* aktivieren.
4. Im Feld *Routing Address* werden die IP-Adressen eingetragen, welche durch den VPN Tunnel man erreichen will.
5. *Source IP Pools* Dieses Feld definiert, welche IP-Adressen dem VPN User an den Virtuellen Adapter zugewiesen werden soll.
6. in den *Tunnel Mode Client Options* können noch Client spezifische Einstellungen vorgenommen werden (Passwort speichern, automatische Verbindung usw.)



New SSL-VPN Portal

Name:

Limit Users to One SSL-VPN Connection at a Time: ☐

Tunnel Mode ☒

Enable Split Tunneling ☒

Routing Address:

Source IP Pools:

Tunnel Mode Client Options

Allow client to save password: ☐

Allow client to connect automatically: ☒

Allow client to keep connections alive: ☒

DNS Split Tunneling: ☐

Host Check: ☐

Restrict to Specific OS Versions: ☐

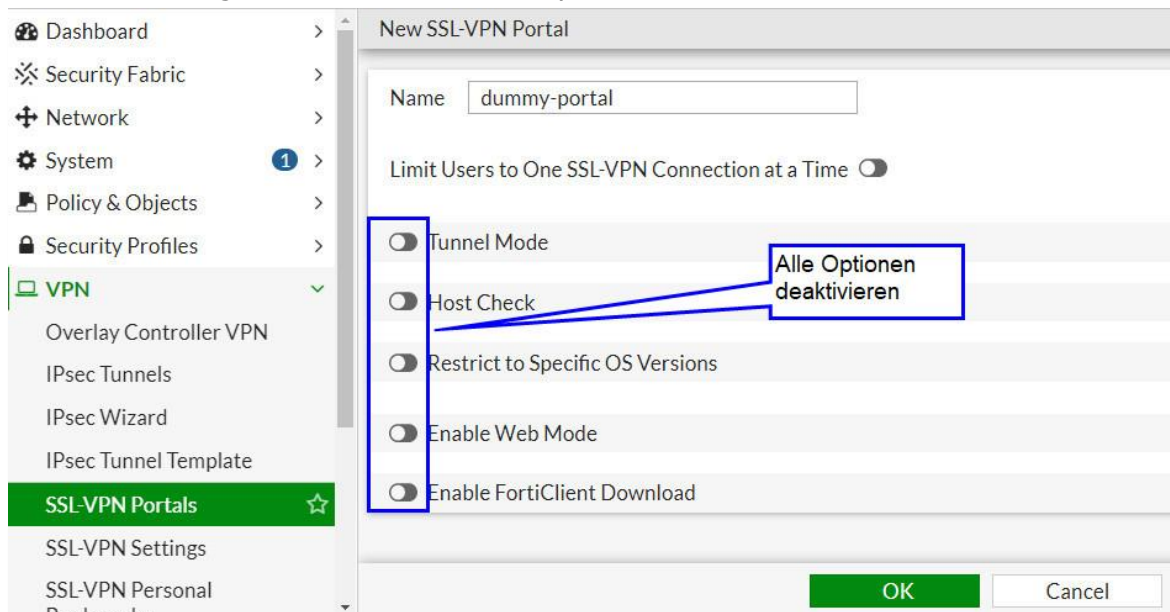
Enable Web Mode ☐

Enable FortiClient Download: ☐

OK **Cancel**

Sobald dieses Portal konfiguriert wurde, brauchen wir noch ein Portal, um alle Anfragen abzufangen, welche nicht definiert wurden. (Ein sogenanntes Dummy Portal) In diesem Portal werden sämtliche Funktionen ausgeschaltet:

1. *Name* der Name des Portals definieren (dummy-portal)
2. Tunnel Mode und Webmode deaktivieren, auch alle anderen Optionen wird empfohlen zu deaktivieren
3. Mit **OK** bestätigen, schon ist das dummy Portal definiert



New SSL-VPN Portal

Name:

Limit Users to One SSL-VPN Connection at a Time: ☐

☐ Tunnel Mode

☐ Host Check

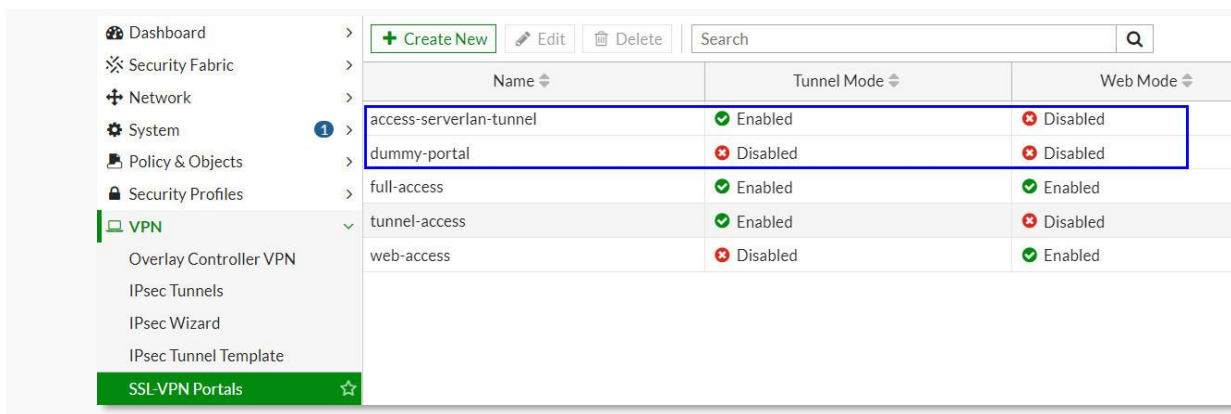
☐ Restrict to Specific OS Versions

☐ Enable Web Mode

☐ Enable FortiClient Download

OK Cancel

Wir sehen jetzt eine Übersicht mit den neu angelegten Portalen, welche Moden ein und ausgeschaltet sind



Name	Tunnel Mode	Web Mode
access-serverlan-tunnel	Enabled	Disabled
dummy-portal	Disabled	Disabled
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

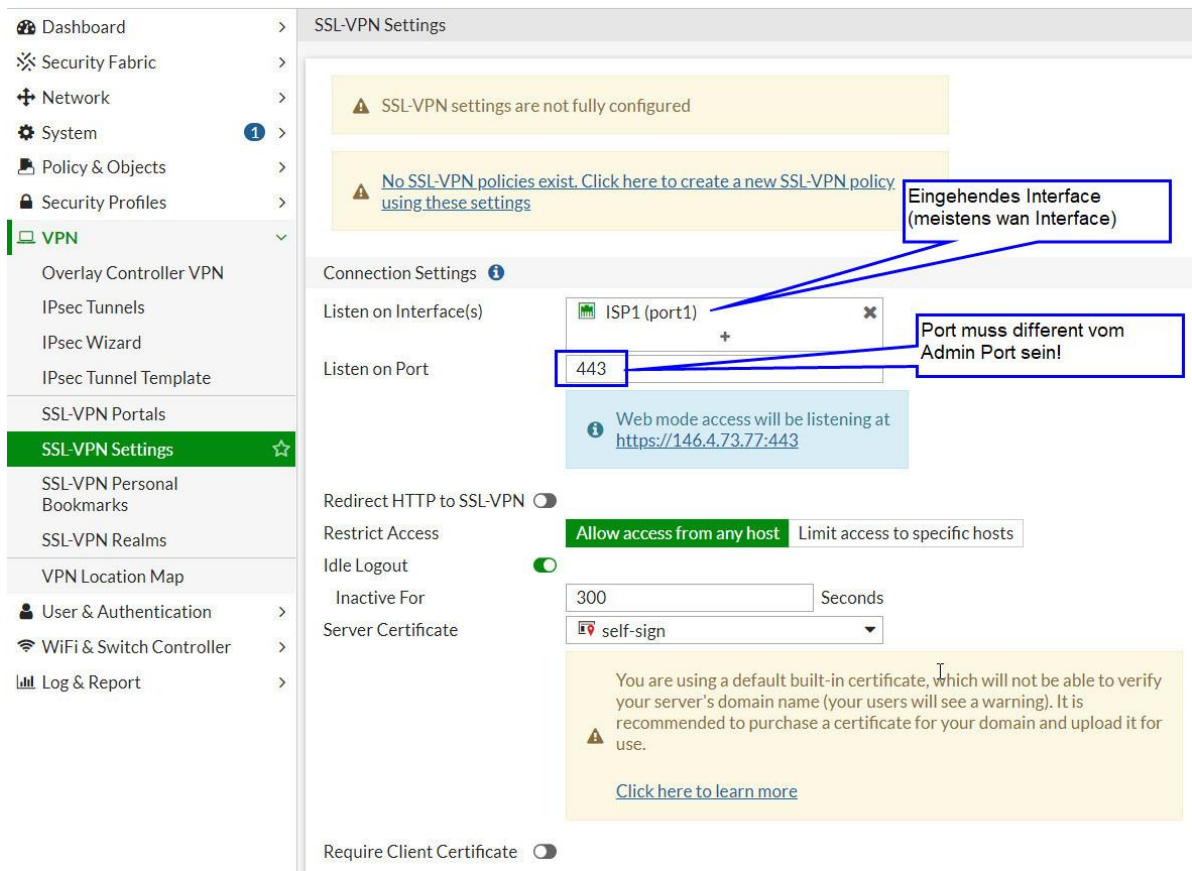
Konfigurieren der SSL-Portale über die CLI:

```
config vpn ssl web portal
    edit "access-serverlan-tunnel"
        set tunnel-mode enable
        set forticlient-download disable
        set auto-connect enable
        set keep-alive enable
        set save-password enable
        set ip-pools "ip-pool-sslvpn-10.10.85.1-254"
        set split-tunneling-routing-address "net-srvlan-10.10.80.0-24"
    next
    edit "dummy-portal"
        set forticlient-download disable
    next
end
```

SSL-VPN Settings

Nun müssen die eigentlichen SSL-VPN Einstellungen konfiguriert werden.

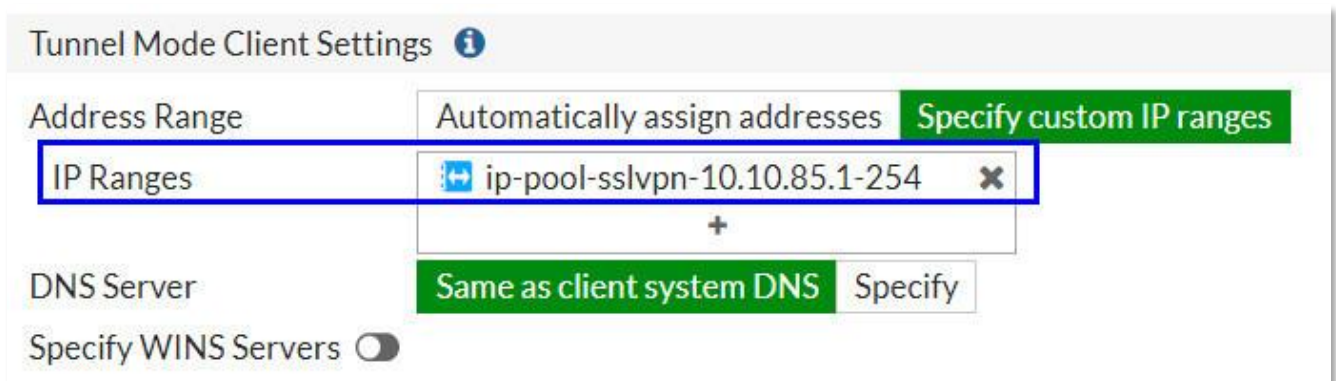
1. *Menu VPN* → *SSL-VPN Settings* anwählen
2. Im *Listen on Interface(s)* werden die Interfaces definiert, auf welches das SSL-VPN Portal angesprochen werden soll
3. Das *Listen on Port* Feld definiert, auf welchen Port das Portal horcht. Wichtig, es muss ein einzigartiger Port auf der anzusprechenden IP-Adresse sein. Es ist darauf zu achten, dass nicht derselbe Port wie der ADMIN Port benutzt wird. Auch sollte man darauf achten, dass dieser Port nicht in einem VIP (Destination Nat) Objekt benutzt wird.
4. Im hellblauen Feld sieht man eine "Vorschau" wie man das Portal über die IP-Adresse erreichen kann:
5. Im Feld *Restrict Access* können Netze definiert werden, von wo her der Zugriff erlaubt ist. Ich empfehle hier *allow access from any host* zu wählen. Wenn man einschränken will, kann man z.B. GEO-IP Benutzen und nur Schweizer IP-Adressen zulassen.
6. *Idle Logout* definiert bei Inaktivität wie lange es geht bis der VPN-Tunnel abgebaut wird (Wert in Sekunden)
7. *Server Certificate* Wenn vorhanden kann hier ein Zertifikat definiert werden



The screenshot shows the 'SSL-VPN Settings' page in the Fortinet GUI. The left sidebar contains a menu with options like Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, Overlay Controller VPN, IPsec Tunnels, IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, SSL-VPN Settings (highlighted), SSL-VPN Personal Bookmarks, SSL-VPN Realms, VPN Location Map, User & Authentication, WiFi & Switch Controller, and Log & Report.

The main content area shows the 'SSL-VPN Settings' configuration. At the top, there are two warning messages: 'SSL-VPN settings are not fully configured' and 'No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings'. Below these, the 'Connection Settings' section is visible. It includes fields for 'Listen on Interface(s)' (set to 'ISP1 (port1)') and 'Listen on Port' (set to '443'). A blue box highlights the port number '443' with the annotation 'Eingehendes Interface (meistens wan Interface)' and 'Port muss different vom Admin Port sein!'. A blue box also highlights the 'Listen on Port' field with the same annotation. Below the port field, a blue box contains the text: 'Web mode access will be listening at https://146.4.73.77:443'. The 'Redirect HTTP to SSL-VPN' toggle is turned off. The 'Restrict Access' section has 'Allow access from any host' selected. The 'Idle Logout' toggle is turned on, with 'Inactive For' set to '300' seconds. The 'Server Certificate' dropdown is set to 'self-sign'. A yellow warning box at the bottom states: 'You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use. Click here to learn more'. The 'Require Client Certificate' toggle is turned off.

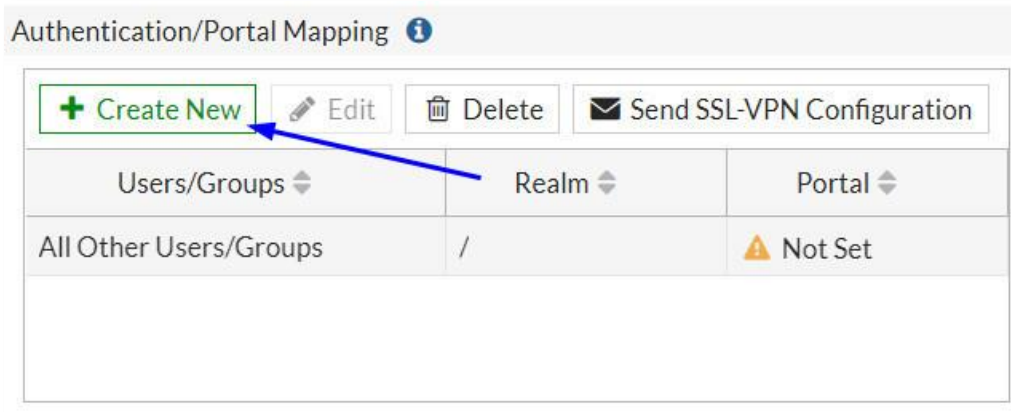
1. Im Feld *Address Range* werden die IP-Adressen und IP Netze definiert, welche über das VPN erreicht werden sollen
2. Um einen selber angelegten IP-Pool zu verwenden muss die Option *Specify custom IP ranges* angewählt werden, danach kann das gewünschte Objekt/Objekte ausgewählt werden.
3. Es kann bei *DNS Server* angegeben werden, ob der Client DNS Server benutzt werden soll oder ob man einen Spezifischen DNS Server für den Client benutzen will.



The screenshot shows the 'Tunnel Mode Client Settings' page. The 'Address Range' section has two tabs: 'Automatically assign addresses' and 'Specify custom IP ranges' (highlighted in green). Below the tabs, the 'IP Ranges' field is highlighted with a blue box and contains the text 'ip-pool-sslvpn-10.10.85.1-254'. The 'DNS Server' section has two tabs: 'Same as client system DNS' (highlighted in green) and 'Specify'. The 'Specify WINS Servers' toggle is turned off.

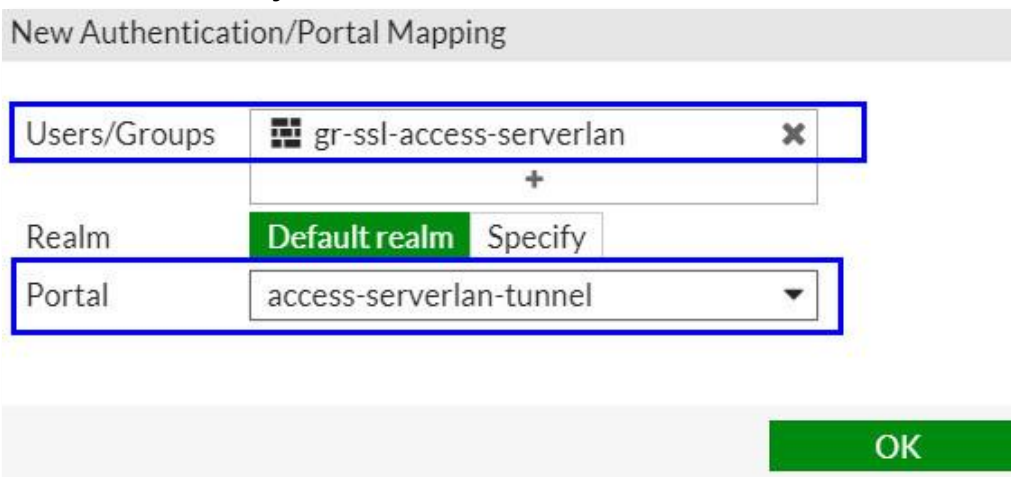
Nun werden die Portale den entsprechenden Usergruppen zugewiesen:

1. im Abschnitt *Authentication/Portal Mapping* auf **+ Create New** ein neues Mapping erstellen



Users/Groups	Realm	Portal
All Other Users/Groups	/	⚠ Not Set

2. die User oder Gruppen auswählen
3. wir haben kein Realm in diesem Szenario definiert, daher können wir das Default realm benutzen.
4. Beim Portal können wir jetzt unser definiertes Portal auswählen

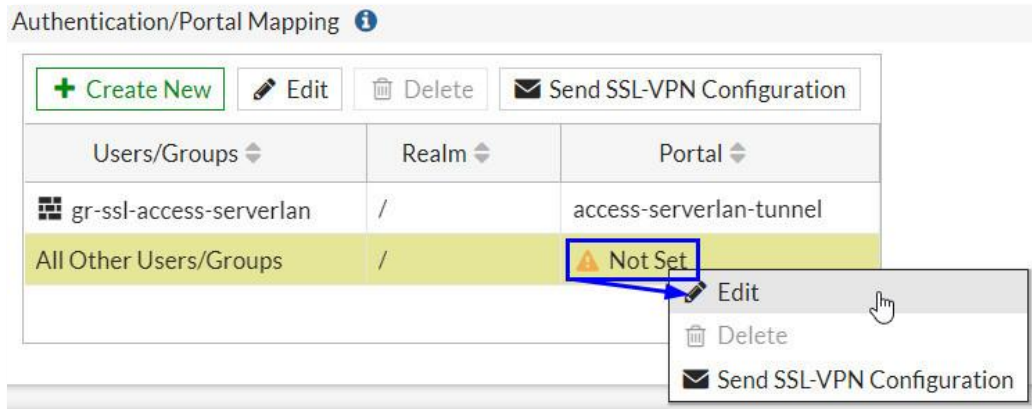


Users/Groups	gr-ssl-access-serverlan
Realm	Default realm
Portal	access-serverlan-tunnel

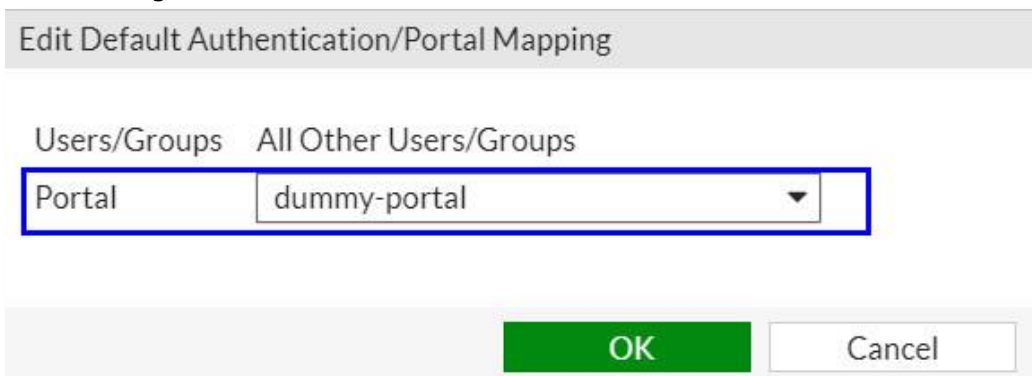
OK

Nun hat es noch eine vordefinierte Aktion, welche alle anderen User und Gruppen betreffen, welche oberhalb nicht definiert wurden. Für diesen Fall haben wir das dummy-Portal angelegt.

1. auf *Not Set* klicken
2. *edit* anwählen



3. Bei Portal das *dummy-portal* auswählen
4. Mit *OK* bestätigen

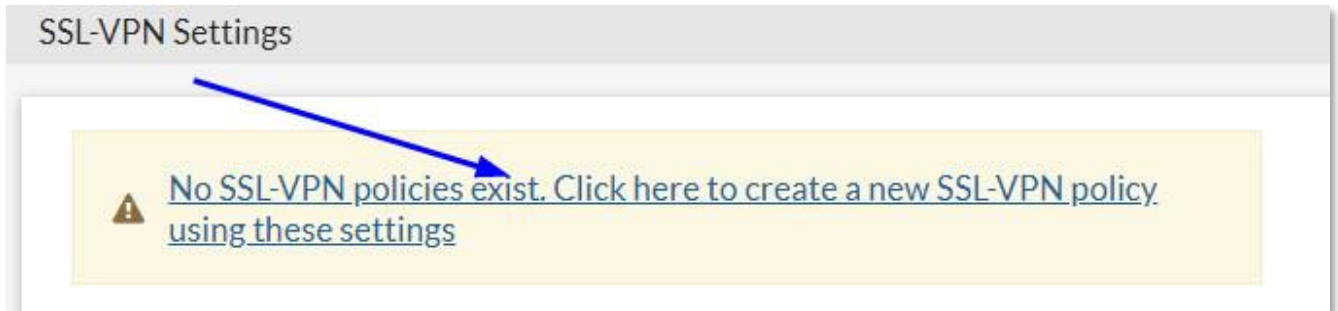


Nun muss man ganz nach oben scrollen und in das hellgelbe Feld klicken. So kann man direkt eine Firewall Policy erstellen

Konfigurieren der SSL-VPN Settings in der CLI:

```
config vpn ssl settings
  set servercert "self-sign"
  set tunnel-ip-pools "ip-pool-sslvpn-10.10.85.1-254"
  set port 443
  set source-interface "port1"
  set source-address "all"
  set source-address6 "all"
  set default-portal "dummy-portal"
  config authentication-rule
    edit 1
      set groups "gr-ssl-access-serverlan"
      set portal "access-serverlan-tunnel"
    next
  end
end
```

Nun muss man ganz nach oben scrollen und in das hellgelbe Feld klicken. So kann man direkt eine Firewall Policy erstellen



Firewall Regeln konfigurieren

1. Beim *Incoming Interface* wird das ssl-vpn Tunnel Interface ausgewählt. Dieses Interface wird von der FortiGate automatisch angelegt :SSL-VPN tunnel Interface (ssl.VDOMNAME)
2. Beim *Outgoing Interface* wird das Interface selektiert, hinter welchem mein zu erreichendes IP-Netzwerk liegt
3. Das 'Source Feld bekommt das IP Pool Objekt und die Gruppe welche für das SSL-VPN benutzt wird.
4. Destination hier wird das Ziel Netz angegeben.
5. Unter Service können die zu erlaubenden Protokole definiert werden
6. Wichtig ist, dass der NAT Schalter deaktiviert wird. Ansonsten wird das Rückrouting zum EndClient nicht mehr funktionieren (wir benutzen dann die Source IP-Adresse des ausgehenden Interfaces)
7. Es können noch die *Security Profiles* nach seinem Konzept definiert werden
8. Bei der Option *Log Allowed Traffic* empfehlen wir auf *All Sessions* zu stellen (dann sehen wir im Log auch alles)
9. darauf achten, dass die Firewall Regel auch aktiviert wird. *Enable this policy* einschalten.

Name	I_SSL-VPN->Serverlan-serverdienste		
Incoming Interface	SSL-VPN tunnel interface (ssl.root)		
Outgoing Interface	server-lan (port3)		
Source	ip-pool-sslvpn-10.10.85.1-254 gr-ssl-access-serverlan +		
Destination	net-srvlan-10.10.80.0-24 +		
Schedule	always		
Service	HTTPS PING RDP +		
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY		
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based		
Firewall / Network Options			
NAT	<input type="checkbox"/>		
Protocol Options	<input checked="" type="checkbox"/> default		
Security Profiles			
AntiVirus	<input type="checkbox"/>		
Web Filter	<input type="checkbox"/>		
DNS Filter	<input type="checkbox"/>		
Application Control	<input type="checkbox"/>		
IPS	<input type="checkbox"/>		
File Filter	<input type="checkbox"/>		
SSL Inspection	<input checked="" type="checkbox"/> no-inspection		
Logging Options			
Log Allowed Traffic	<input checked="" type="checkbox"/> Security Events <input checked="" type="checkbox"/> All Sessions		
Generate Logs when Session Starts	<input type="checkbox"/>		
Comments	Write a comment... 0/1023		
Enable this policy <input checked="" type="checkbox"/>			

VPN Regeln sollten immer möglichst weit oben im Policy Set angefügt werden. Die Reihenfolge der Policies kann am besten in der *By Sequence* Ansicht angeschaut werden.

+ Create New	Edit	Delete	Policy Lookup	Search		Interface Pair View	By Sequence
Name	From	To	Source	Destination	Schedule	Service	Action
SSL-VPN Zugang							
I_SSL-VPN->Serverlan-serverdienste	SSL-VPN tunnel interface (ssl.root)	server-lan (port3)	gr-ssl-access-serverlan ip-pool-sslvpn-10.10.85.1-254	net-srvlan-10.10.80.0-24	always	HTTPS PING RDP	✓ ACCEPT

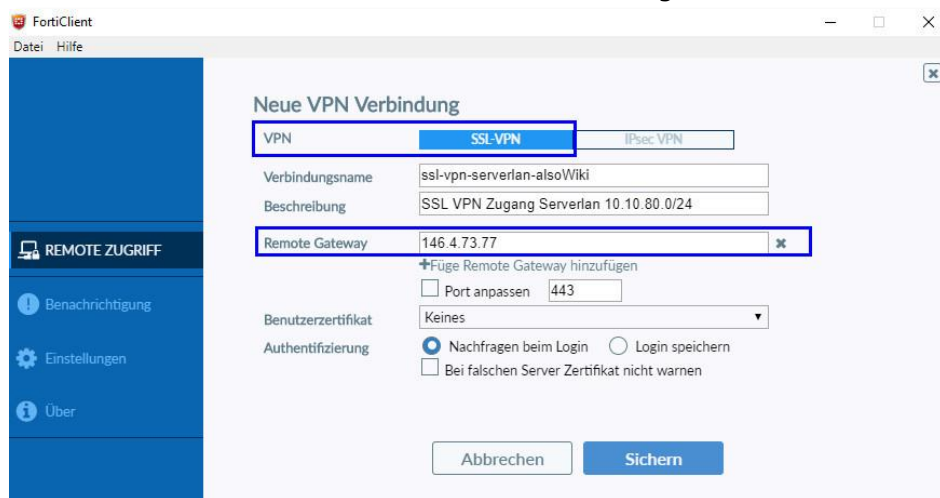
Firewallregel in der CLI konfigurieren:

```
config firewall policy
  edit [POLICY_ID]
    set name "I_SSL-VPN->Serverlan-serverdienste"
    set srcintf "ssl.root"
    set dstintf "port3"
    set srcaddr "ip-pool-sslvpn-10.10.85.1-254"
    set dstaddr "net-srvlan-10.10.80.0-24"
    set action accept
    set schedule "always"
    set service "HTTPS" "PING" "RDP"
    set logtraffic all
    set groups "gr-ssl-access-serverlan"
  next
end
```

VPN Client Konfigurieren

Beim FortiClient eine neue Verbindung erstellen: Auf das Zahnrad  klicken und *neue Verbindung* auswählen

1. VPN auf SSL-VPN stellen (wir haben eine SSL-VPN Verbindung auf der FortiGate konfiguriert)
2. Verbindungsname und Beschreibung nach gutdünken konfigurieren
3. Beim Remote Gateway wird die Domäne oder die IP Adresse der FortiGate angegeben auf welcher das SSL-VPN Portal erreichbar ist
4. Port anpassen falls man den SSL-VPN Listen Port angepasst hat, muss hier der entsprechende Wert konfiguriert werden
5. Falls ein Benutzer Zertifikat für die Authentifizierung konfiguriert wurde, kann das im Feld Benutzerzertifikat ausgewählt werden.
6. Authentifizierung hier kann definiert werden, ob die Logging Daten gespeichert werden soll. (Kann auf der FortiGate aber unterbunden werden)
7. auf Sichern und schon ist das VPN auf dem Client konfiguriert.

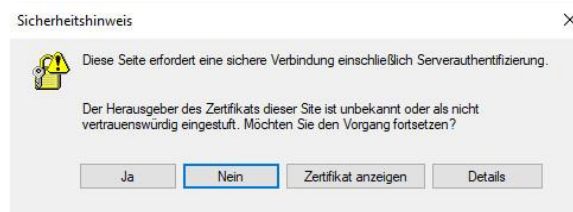


Wenn die VPN Verbindungsoptionen konfiguriert ist, kann man sich mit dem VPN verbinden, indem man auf den Button *Verbinden* klickt.

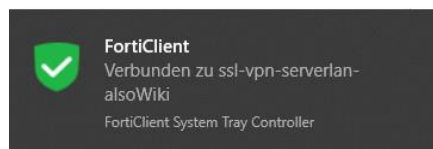


The image shows a VPN connection interface. At the top, there is a graphic of a globe with a laptop and a padlock icon. Below this, there are three input fields: 'VPN Name' with a dropdown menu showing 'ssl-vpn-serverlan-alsoWiki', 'Benutzername' with the text 'user1', and 'Passwort' with masked characters '*****'. At the bottom, there is a blue button labeled 'Verbinden'.

Wenn das Default Zertifikat von der FortiGate benutzt wird, gibt es einen Hinweis, dass dieses Zertifikat nicht als vertrauenswürdig eingestuft wird. Diese Meldung kann man mit *Ja* bestätigen.



Wenn Username und Passwort richtig sind, wird sich der Client am VPN anmelden. Wir bekommen folgende Meldung:

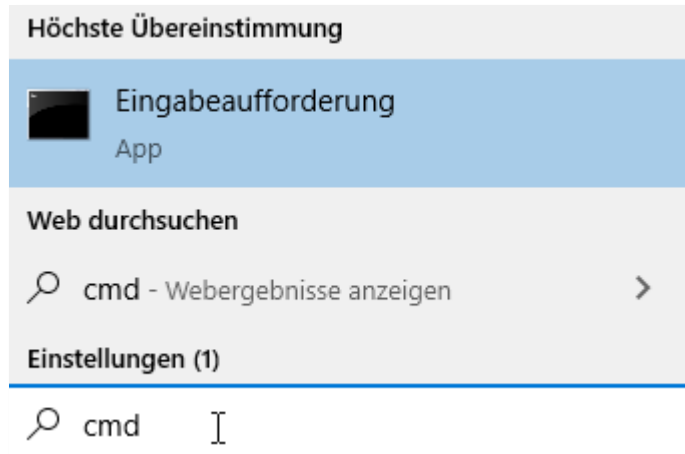


Auf dem Client selber sehen wir, wie lange der User verbunden ist, und wieviele Daten er in dieser Session überträgt. Weiter sehen wir auch, die IP-Adresse welche er von der FortiGate zugewiesen bekommen hat.



Kontrollen und Logs:

Wir können auf dem Client über das Eingabe Fenster von Windows CMD eingeben.



Es öffnet sich das schwarze Eingabe Fenster.

In In diesem Eingabefenster kann man den Befehl `ipconfig` eingeben. Nun werden alle Netzwerkkarten und Adapter aufgelistet und welche IP Adresse darauf konfiguriert oder zugewiesen wurden angezeigt. Unser Adapter vom Fortinet VPN heisst Fortinet SSL VPN Virtual Ethernet Adapter nach diesem müssen wir suchen. Wir sehen, dass wir da die IP Adresse `10.10.85.1` zugewiesen bekommen haben.

```
Ethernet-Adapter Ethernet 3:

Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . : Fortinet SSL VPN Virtual Ethernet Adapter
Physische Adresse . . . . . : 00-09-0F-AA-00-01
DHCP aktiviert. . . . . : Nein
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::a81d:df04:bc17:c206%3(Bevorzugt)
IPv4-Adresse . . . . . : 10.10.85.1(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.255
Standardgateway . . . . . :
DHCPv6-IAID . . . . . : 83888399
DHCPv6-Client-DUID. . . . . : 00-01-00-01-21-C1-5D-26-1C-1B-0D-6A-27-80
DNS-Server . . . . . : 10.60.60.2
NetBIOS über TCP/IP . . . . . : Aktiviert
```

Da wir einen Split Tunnel konfiguriert haben, sehen wir auch, dass nur unser **Netz 10.10.80.0/24 (Gelb)** in den Tunnel geroutet wird.

Die Default Route **0.0.0.0/0 (Magenta)** zeigt weiterhin auf den lokalen Gateway 10.60.60.2

Die Routingtabelle kann man mit dem Befehl `route print` anzeigen lassen. Für diese Aktion muss man das CMD Programm aber als Administrator ausführen!

```
C:\WINDOWS\system32>route print

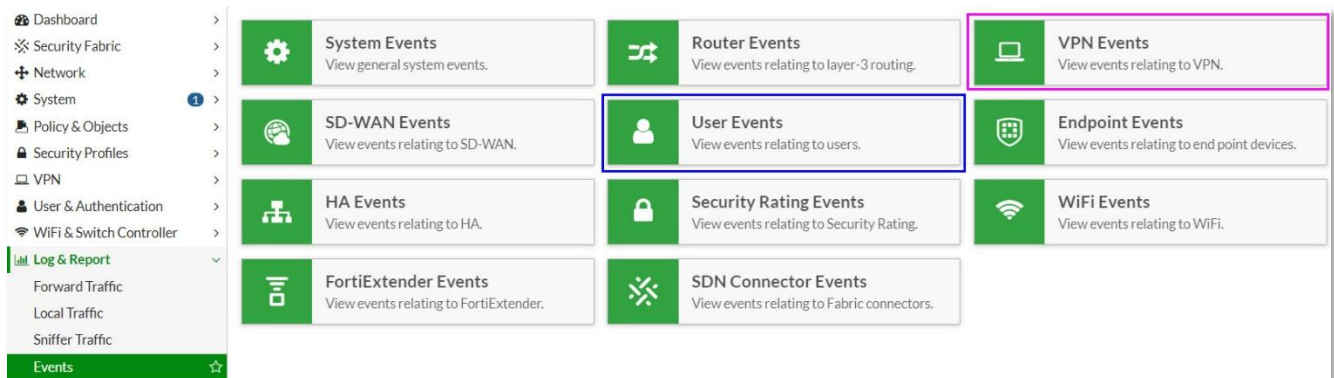
=====
Schnittstellenliste
14...00 09 0f fe 00 01 .....Fortinet Virtual Ethernet Adapter (NDIS 6.30)
3...00 09 0f aa 00 01 .....Fortinet SSL VPN Virtual Ethernet Adapter
15...1c 1b 0d 6a 27 80 .....Intel(R) Ethernet Connection (2) I219-V
13...88 d7 f6 bc 28 c3 .....ASUS Wireless PCI-E Adapter
20...88 d7 f6 bc 28 c3 .....Microsoft Wi-Fi Direct Virtual Adapter #2
1.....Software Loopback Interface 1
=====

IPv4-Routentabelle
=====
Aktive Routen:
```

Netzwerkziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik
0.0.0.0	0.0.0.0	10.60.60.2	10.60.60.100	25
10.10.80.0	255.255.255.0	10.10.85.2	10.10.85.1	1

Auf der FortiGate können wir das Ganze im Event Log anschauen gehen:

Zum Event Log gelangt man folgenermassen: *Log & Report* → *Events* → *entsprechende Kategorie auswählen*







Für das User Eventlog:

Log & Report → *Events* → *User Events (Blau)*




Date/Time	Level	User	Action	Message
2020/11/02 09:09:37		 user1	auth-logon	User user1 added to auth logon

Für das VPN Eventlog

Log & Report → Events → *VPN Events (Magenta)*

Date/Time	Level	Action	Status	Message	VPN Tunnel
2020/11/02 09:09:37		tunnel-up		SSL tunnel established	
2020/11/02 09:09:37		ssl-new-con		SSL new connection	
2020/11/02 09:09:36		tunnel-up		SSL tunnel established	
2020/11/02 09:09:36		ssl-new-con		SSL new connection	

Um eine Detaillierte Ansicht zu bekommen auf das entsprechende Event klicken:
Hier sehen wir den User, die IP Adresse welcher der Client zugewiesen bekommen hat usw.

Date/Time	Level	Action	Status	Message	Log Details
2020/11/02 09:09:37		tunnel-up		SSL tunnel established	<div> <div>General</div> <div> Date 2020/11/02 Time 09:09:37 Virtual Domain root Log Description SSL VPN tunnel up </div> </div> <div> <div>Source</div> <div> User  user1 Group gr-ssl-access-serverlan </div> </div> <div> <div>Destination</div> <div>Destination Host N/A</div> </div> <div> <div>Action</div> <div> Action tunnel-up Reason tunnel established </div> </div> <div> <div>Security</div> <div> Level  </div> </div> <div> <div>Event</div> <div> Remote IP 85.136.170.6 Tunnel ID 545837470 Tunnel IP 10.10.85.1 Tunnel Type ssl-tunnel Message SSL tunnel established </div> </div> <div> <div>Other</div> <div> LogID 0101039947 Type event Sub Type vpn Log event original timestamp 1604304577820484600 Timezone +0100 </div> </div>